FILED UNDER SEAL PURSUANT TO THE E-GOVERNMENT ACT OF 2002

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF THE RESIDENCE LOCATED AT:

[redacted]
Chesapeake, Virginia 23325

Case No. 2:16ms75

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Harald S. Julsrud III, being first duly sworn state:

1. I am a Special Agent of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Office of the Assistant Special Agent in Charge (ASAC), Norfolk, Virginia. I have been so employed since December 2007. Your Affiant is currently assigned to HSI Norfolk Homeland Security and Child Exploitation Group. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center, the HSI Cyber Crimes Center, conferences related to the aforementioned subject matter, and everyday work relating to conducting these types of investigations. In addition to training in the area of child pornography and child exploitation, your affiant has had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Since 2010, I have also been a Computer Forensics Agent with HSI, and as part of my duties, have supported numerous criminal investigations related to child exploitation. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for [redacted] Chesapeake, Virginia, 23325 (the SUBJECT PREMISES), described in Attachment A, for the items specified in Attachment B hereto.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other HSI Special Agents, other law enforcement agents and on my investigation of this matter. Because this affidavit is being submitted for the limited purpose

of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4), receipt and possession/access with intent to view child pornography, is located at [redacted] Chesapeake, Virginia, 23325.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4), which make it a crime to receive and possess/access with intent to view child pornography.

PERTINENT FEDERAL CRIMINAL STATUTES

6. 18 U.S.C. § 2252(a)(2) provides that any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct, shall be punished.

7. 18 U.S.C. § 2252(a)(4) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer;

DEFINITIONS

8. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. graphic records or representations;
b. photographs;
c. pictures;
d. images, and
e. aural records or representations.

9. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical,

electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

10. The terms "minor" and "sexually explicit conduct" are defined in 18 U.S.C. Section 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

a. Sexual intercourse, including genital genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex;
b. Bestiality;
c. Masturbation;
d. Sadistic or masochistic abuse; or
e. Lascivious exhibition of the genitals or pubic area of any person.

11. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

12. The term "Computer" as used herein is defined pursuant to Title 18 U.S.C. Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

13. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

14. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

15. The term "Universal Resource Locator" (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific

computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

16. The term "Internet Protocol Address" (IP Address): This term refers to the fact that every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses; static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

17. The term "Internet Service Provider" (ISPs): This term refers to individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

18. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

19. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. Title 18 U.S.C. Section 2510(15).

20. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." Title 18 U.S.C. Section 2711.

21. "Electronic Communications System" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Title 18 U.S.C. Section 2510(14).

22. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. Title 18 U.S.C. Section 2510(8).

23. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Title 18 U.S.C. Section 2510(17).

24. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

25. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

26. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Your affiant, based on my experience and conversations with Computer Investigative Specialists who have been trained in the seizure, examination and retrieval of data from personal computer systems and related media, knows that searching and seizing information from computer systems often requires agents to seize all electronic storage devices to be searched later in a laboratory or other controlled environment.

28. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and USB, thumb or flash drives) can store enormous quantities of information. For instance, a single 2 gigabyte hard drive may contain the electronic equivalent of hundreds of thousands of pages of

LRL

double spaced text. However, unlike the search of documentary files, computers store data in files that are often not easily reviewed. Additionally, a suspect may try to conceal criminal evidence by storing files in random order and/or with deceptive file names. This may require the examiner to examine all the stored data to determine which particular files are evidence or instrumentalities of the crime. This sorting process can take weeks or months, depending on the volume of data stored.

29. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skills and a properly controlled environment. The vast array of computer hardware and software available requires even computer examiners to specialize in some systems and applications, so it is difficult to know before a search which computer investigative specialist is qualified to analyze the system and its data. In any event, the investigative specialist will use certified forensic tools and data search protocols that are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system such as a booby trap), a controlled environment is essential to its complete and accurate analysis.

30. An important step that is ordinarily part of an examiner's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

31. Through my discussions with law enforcement officers who specialize in the investigation of child pornography, and of subjects who use the Internet and e-mail to gain access to child pornography, I have learned that individuals who use such technology are often child pornography collectors who download images and videos of child pornography. Moreover, I have learned that many subjects have saved numerous images to their hard drive, thumb drive, disks or CDs, and have kept that material for long periods of time. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in

LRL

person, in photographs, in other visual media or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

32. Based upon the information officially supplied to me by other law enforcement officers, your affiant knows the following:

33. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They have also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

34. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution and storage.

a. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as methods that have been used in the past.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone lines or other cable lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Microsoft and America Online, which allow subscribers to access their network services via connection through an Internet broadband provider or by dialing a local number and connecting via a telephone modem.

LRL

c. These service providers allow electronic mail ("e mail") service between subscribers and between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web, hence they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time using a mode of communication called instant messaging, or "IM." When logged into an IM service, users can search for other users based on the information that the other users have supplied, and they can send those users messages or initiate a chat session. Chat sessions can occur in multiple person groups, or in private one on one sessions. Most IM services also allow files to be transferred between users, including image files.

d. These communications structures are ideal for the child pornography collector. The open and anonymous communication allows users to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collectors can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

e. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file transfer protocols (FTPs), or via news group postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer is a preferred method of distribution of child pornographic materials.

35. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store

HDD3

LBL

thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

36. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space; that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION INTO "BULLETIN BOARD A"

37. In September 2015, the HSI Cyber Crimes Center, Child Exploitation Investigations Unit (C3/CEIU) became involved in an ongoing child pornography investigation. At the present time, this investigation involves multiple individuals, believed to be residing across the United States as well as abroad, who are members of an Internet-based bulletin board (hereafter referred to as BULLETIN BOARD A) dedicated to the advertisement, distribution and production of child pornography. BULLETIN BOARD A has over 1500 "approved users[1]," who actively post new content and engage in online discussions involving the sexual exploitation of minors.

38. BULLETIN BOARD A has various sections containing forums and sub forums in which members post messages and/or images for other members. For example, there is a section labeled "Girls," and within this section there are the following forums: "Model/Producer

[1] This figure is taken from a posting by one of BULLETIN BOARD A's administrators. NOTE: Administrators manage the technical details required for the running of the site. As such, they may promote members, set rules, create sections and act as moderators.

HAB

LRL

section;" "Pre-teen Hardcore;" Pre-teen Softcore/Non-nude;" "Teen/Jailbait;" "Cam;" "Fetishes;" "Babies and toddlers" and "Requests."

39. In October of 2015 C3/CEIU began working with the Department of Justice, Child Exploitation and Obscenity Section (CEOS), High Technology Investigative Unit (HTIU). Since that time, HTIU has captured content contained on BULLETIN BOARD A. C3/CEIU personnel has reviewed this content and observed various postings by board members. One such post was found within the section titled "Girls," forum "Pre-teen Hardcore," sub-forum "Videos." This post was made to the board by a member (hereafter referred to as BOARD MEMBER A) on October 26, 2015, and it consisted of the title: "Hot latin doggyfuck" followed by a preview still image file containing several smaller still images from the video in question, affording the user the opportunity to pre-view the content of said video. In addition, the posting provided the filename: "(~pthc center~)(opva)(2013) Hot latin doggyfucking WP_20130324_052315Z," the file size: 7.70 MB, the Archive name: myuimy5r6yu5e433e.7z, the Duration: 00:00:49, the Download link, Password, and the Download key, among other information. If the user were to hover their cursor over the download link, the post would provide the full download link: http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html. This post also contained a password, which users could input to access and open the content of the file associated with that unique URL.

40. HTIU downloaded the file titled "(~pthc center~)(opva)(2013) Hot latin doggyfucking WP_20130324_052315Z" from the above listed URL. This file was encrypted, but by using the password provided in the post detailed above, the file could be opened and viewed. C3/CEIU personnel has provided this file to me, and I have reviewed its contents. The video file consists of what appears to be an adult male engaged in sexual activity with what appears to be an underage minor. Specifically, the video depicts a scene recorded from above, showing what appears to be an adult male from the waist down, with his pants pulled down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor's back and buttocks. The video file is 49 seconds in duration and contains audio.

BULLETIN BOARD A's MEMBERS' USE OF FILE SHARING SERVICES

41. Law enforcement has determined that these unique URLs, like the one mentioned above, which are posted by members of Bulletin Board A and which provide board members access to files depicting minors engaging in sexually explicit conduct, are hosted by several different cloud-based storage services. One of the storage services used by Bulletin Board A's members, hereafter referred to as FSS (File Sharing Site), offers online file hosting and sharing services. As stated on FSS's homepage, located at http://[FSS].com/:

> In [FSS].com You can upload & share any data such as video, music, images and even compressed rar[2] files and any other kinds of documents Freely. Downloading Your

[2] A RAR file is a form of compressed archive which provides both archiving and compression, and it allows for multiple files that have been reduced in size to be contained inside a single RAR file.

HSI 3

BL

friends files from any kind freely with direct link. Hope you enjoy our online file hosting and sharing services.

42. Though FSS does offer online file hosting and sharing for free, it also offers different service packages for monthly fees. These service packages offer enhanced services such as "Unlimited File Access" and "2 Months Support."

43. FSS's Terms of Service page, at http://[FSS].com/tos.html, explain FSS's expectations of its users, and what users should expect from FSS. The following is taken from FSS's Terms of Service page:

> This [FSS] Service Agreement (the "Agreement") describes the terms and conditions on which [FSS] ("we") offer services to you ("User"). By using our services, User agrees to be bound by the following terms and conditions: We reserve the right to disable direct linking on user accounts that are using excessive bandwidth or otherwise abusing the system.
>
> Pornography, nudity, sexual images and any kind offensive images or videos are prohibited. Copyrighted material are also strictly prohibited. We reserve the right to decide appropriate content and can delete images or videos at any time without User notification.
>
> Users must agree to comply with all laws which apply to their location, including copyright and trademark laws. Images, videos and files that violate copyrights or trademarks are not allowed. If someone has an infringement claim against you, you will be asked to remove the copyrighted file until the issue is resolved. If there is a dispute between participants on this site, [FSS] is under no obligation to become involved.
>
> [FSS] is not liable for your images, videos or files or any lost business due to the unavailability or loss of the website. We make no claims of future reliability in serving, hosting or storing your images, videos or files.
>
> [FSS] is committed to cooperate with any and all legal authorities if an investigation should arise.

44. Based upon the information detailed above, law enforcement had reason to believe that FSS's service was used by members to store files containing child pornography and make them accessible to other members. FSS provided this service using computer servers owned, maintained, controlled or operated by a provider whose name is known to Law Enforcement. The investigation has revealed that this provider has headquarters located in the United States.

45. On December 07, 2015, the United States District Court of the District of Columbia issued an Order pursuant to Title 18 United States Code §2703(d), directing FSS to disclose certain records and other information relating to a list of unique URLs that contained files which had been viewed by law enforcement and determined that each depicted minors

engaging in sexually explicit conduct. This Order was sent to FSS and in response to that Order, FSS produced business records which included the dates, times and IP addresses connected to the downloading of the file content associated with the URLs specified in the application for the Order.

IDENTIFICATION OF THE SUBJECT PREMISES

46. The following records were provided by FSS and were associated with the access, download and/or attempted download of file content associated with the following unique URL http://[FSS].com/mkj6j8qjxixb/myuimy5r6yu5e433e.7z.html.

47. On October 28, 2015, at 5:51:47 PM (17:51:47) Eastern Daylight Time [EDT], IP address 70.161.118.157 was used to download, and/or attempted to download, file content associated with that URL, which as detailed above, consisted of a 49 second video file depicting what appears to be an adult male from the waist down, with his pants pulled down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor's back and buttocks.

48. Using publically available search tools, law enforcement determined that IP address 70.161.118.157 was controlled by Internet Service Provider (ISP) Cox Communications, Inc. on the date and time in question.

49. On or about December 15, 2015, a Department of Justice subpoena was issued to Cox Communications, Inc. requesting subscriber information relating to the use of IP address on October 28, 2015 at 17:51:47 EDT. On or about January 06, 2016, Cox Communications, Inc. produced business records indicating the following subscriber information:

Billing Name: [redacted] Reece
Billing Address: [redacted] Chesapeake, VA 23325-2801

50. A check of publicly available databases also revealed that [redacted] Reece may be married to Larry Reece.

51. Surveillance of the SUBJECT PREMISES on or about February 01, 2016, revealed parked in the SUBJECT PREMISES driveway a Ford Ranger. Records checks indicated that this vehicle is registered to Miscellaneous and Ornamental Metals. Further research indicates that the listed president of the business is Lawrence or Larry Reece. The listed business address is [redacted], Virginia Beach, VA 23451. Attempts to locate an actual structure associated with this business at the listed address have so far proved unsuccessful.

52. Surveillance of the SUBJECT PREMISES on or about February 16, 2016, revealed that parked in the SUBJECT PREMISES driveway was a Jeep Wrangler. Records checks indicated that this vehicle is registered to an individual named Larry James Reece II, date of birth: xx/xx/83, and an individual named [redacted] Reece, date of birth: xx/xx/84.

53. A check with the Virginia Division of Motor Vehicles on or about February 17, 2016, revealed that an individual named Larry James Reece II and an individual named Amberly Austin Reece have a vehicle (the Jeep Wrangler) registered in both names at the SUBJECT PREMISES.

54. Surveillance of the SUBJECT PREMISES on or about February 19, 2016, revealed that parked in the SUBJECT PREMISES driveway was a Subaru WRX. Records checks indicated that this vehicle is registered to an individual named Larry James Reece, date of birth: xx/xx/49.

CONCLUSION

55. Based on the aforementioned factual information, your affiant respectfully submits that probable cause exists to believe that a computer user located at [redacted] Chesapeake, VA 23325, received and/or attempted to receive child pornography, as well as possessed and/or attempted access with intent to view child pornography via the listed e-mail account, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4), which prohibit the knowing receipt of visual depictions of and involving the use of a minor engaging in sexually explicit conduct and possession of or access with the intent to view one or more matters containing visual depictions of and involving the use of a minor engaging in sexually explicit conduct.

56. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within [redacted] Chesapeake, VA 23325. Accordingly, I request that a warrant be issued authorizing your affiant, with assistance from additional HSI agents and other law enforcement personnel, to search [redacted] Chesapeake, VA 23325, for the items specified in Attachment B.

FURTHER AFFIANT SAYETH NOT.

Harald S. Julsrud III, Special Agent
Department of Homeland Security
Homeland Security Investigations
Norfolk, VA

SUBSCRIBED and SWORN before me on this 5th of April, 2016.

UNITED STATES MAGISTRATE JUDGE

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT

BY _____
DEPUTY CLERK